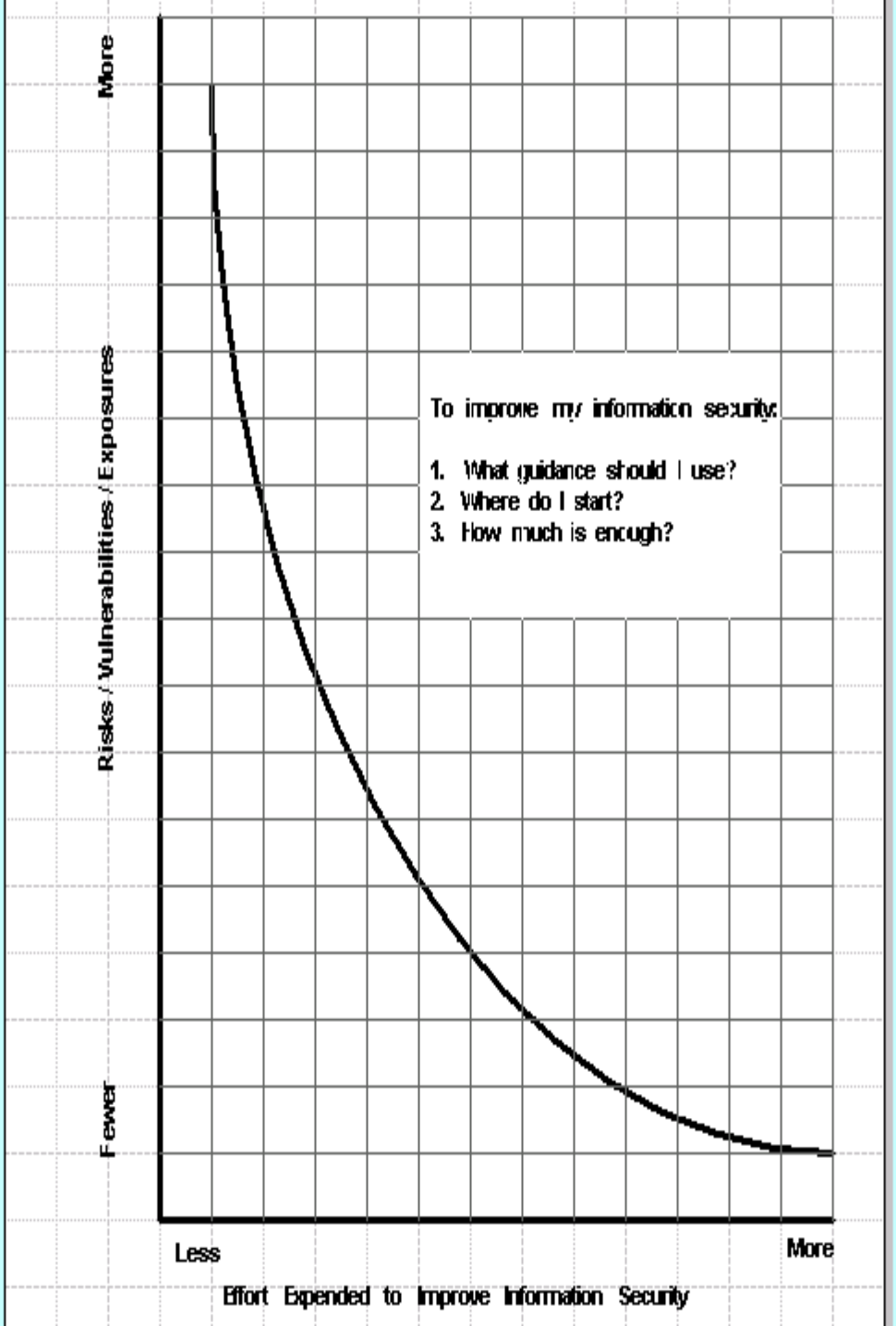
Managing the Risks Related to IT Security

Clint Kreitner

the CENTER for INTERNET SECURITY

Managers continue to ask:

- What do I need to do?
- How much is enough?
- Who can I trust?
- How can I resolve the conflicting advice I’m receiving from “the experts”?
- Why do I have to pay consultants so much for one-off solutions to my IS needs?


More
Risks / Vulnerabilities / Exposures
Fewer
To improve my information security:
1. What guidance should I use?
2. Where do I start?
3. How much is enough?
Less
More
Effort Expended to Improve Information Security

We know that IS involves:

- People
- Process
- Technology

What's the problem? -- Plenty of IS guidance is available

- Principles-based IS Management
- Controls-based IS Management
- IS Management for Specific Sectors
- IS Governance Guides
- Legal/Regulatory Enforcement Guides
- Risk Management Guides
- Technical Control Guides

Examples of Currently Available IS guidance:

- High level principles-based guidance
  - OECD and GAISP
- Mid-level controls-based guidance
  - ISO 17799
  - Trust Services (AICPA)
  - CobIT (ISACA)
  - Standards of Good Practice (ISF) (UK)
  - NIST 800 Series Publications

Currently Available IS guidance (Cont'd):

- "Fundamentals" guidance
  - VISA's Digital Dozen
- Detailed technical controls guidance
  - CIS Consensus Benchmarks and Scoring Tools
  - NSA, DISA, NIST, and some vendors

Security Controls (NIST Pub 800-53)

- Management Controls
  - Controls that address the security management aspects of the IT system and the management of risk for the system
- Operational Controls
  - Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems)
- Technical Controls
  - Controls that address security mechanisms **contained in and executed** by the computer system

Survey of IS Guidance by CISWG Phase I

- Corporate Information Security Working Group (CISWG)
- Convened Fall 2003 by Rep Adam Putnam (R-Fla), Chairman, Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census, Government Reform Committee, US House of Representatives
- Report issued March 2003
  - http://reform.house.gov/TIPRC/

CISWG I Conclusions about available guidance

- Expressed at widely varying levels of abstraction
- Structurally disconnected/fragmented
- Lacking links between principles and related controls
- Not readily scaleable for different types and sizes of organizations
- Developed and promoted by different professional communities often vying for position and recognition, each using its own taxonomy and terminology to describe the same knowledge space
- Much of it is not actionable without significant additional elaboration
- Detailed technical controls have been largely ignored

Goals of CISWG Phase II (Fall 2004)

- Refine the CISWG I IS Program Elements
- Develop Metrics Supporting the Program Elements
- Provide guidance that is
  - Generic across different organizational sizes & types
  - Comprehensive
  - Actionable (can be implemented immediately)

CISWG II

- IS Program Elements
- Supporting Metrics

IS Program Elements – Governing Board

- (1) Establish Risk Thresholds for Critical Information Assets and Information-dependent Functions and Objectives
- (2) Establish Broad IS Program Principles and Assign Senior Management Accountabilities for IS
- (3) Protect Stakeholder Interests Dependent on IS

IS Program Elements – Governing Board

- (4) Ensure Appropriate IS Requirements for Strategic Partners and Vendors
- (5) Comply with External IS Requirements (e.g. Sarbanes-Oxley, HIPAA, GLB)
- (6) Establish Requirements for Internal and External Audits of the IS Program
- (7) Specify the IS Metrics to be Reported to the Board

IS Program Elements - Management

- (8) Establish IS Management Policies and Controls and Monitor Compliance
- (9) Assign IS Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges
- (10) Assess Information Risks & Actively Manage Risk Mitigation

IS Program Elements - Management

- (11) Ensure Implementation of IS Requirements for Strategic Partners and Vendors
- (12) Identify and Classify Information Assets
- (13) Ensure Business Continuity
- (14) Approve Information Systems Architecture during Acquisition, Development, Operations, & Maintenance

IS Program Elements - Management

- (15) Protect the Physical Environment
- (16) Ensure Internal and External Audits of the IS Program with Timely Follow-up
- (17) Specify the IS Metrics to be Reported to Management

IS Program Elements - Technical

- (18) User Identification and Authentication
- (19) User Account Management
- (20) User Privileges
- (21) Configuration Management
- (22) Event and Activity Logging and Monitoring
- (23) Communications, Email, & Remote Access Security

IS Program Elements - Technical

- (24) Malicious Code Protection, including Viruses, Worms, and Trojans
- (25) Software Change Management, including Patching
- (26) Firewalls
- (27) Data Encryption
- (28) Backup and Recovery
- (29) Incident and Vulnerability Detection and Response
- (30) Specify the Technical Metrics to be Reported to Mgmt

Why Metrics?

- What gets measured, gets done
- Metrics are about:
  - Transforming policy into action
  - Measuring performance
  - Motivating human behavior
- Visible scores motivate behavior in a positive way
  - We all want to succeed
  - We want to compare favorably with our peers

Metrics can be:

- General or detailed
- Qualitative or quantitative
- Process or outcome oriented

Generally the best metrics are:

- Quantitative (capable of numeric valuation)
- Outcome oriented
  - An unacceptable value of an outcome metric will invariably suggest that the organizational process that produced the outcome is in need of improvement

Examples: Security Awareness & Training

- The organization has an Employee Security Awareness and Training Program (yes/no)
- # of Employees who have completed the ESA&TP
- % of Employees who have completed the ESA&TP
- % of Employees who have passed a test after completing the ESA&TP

Example – Security Awareness & Training

- % of employee position descriptions with listing of IS skills required by their position
- % of employees who possess the IS skills required by their position

Virtues of good metrics

- They inspire drill-down questions
- They imply that certain relevant factors have been given consideration
- They use data that is readily available rather than requiring elaborate and costly data collection efforts

CISWG II Example – Governing Board

- (1) Establish Risk Thresholds for Critical Information Assets and Information-dependent Functions and Objectives
  - Percentage of key information assets for which a comprehensive strategy has been implemented to reduce IS risks to acceptable thresholds

CISWG II Example – Governing Board

- (3) Protect Stakeholder Interests Dependent on IS
  - Percentage of security incidents that caused damage beyond established risk thresholds to the organization's assets, objectives, or functions
  - Percentage change from the last reporting period in the number of incidents that caused damage beyond established risk thresholds

CISWG II Example – Governing Board

- (6) Establish Requirements for Internal and External Audits of the IS Program
  - Percentage of required internal and external audits completed and reviewed by the Board
  - Percentage of audit findings that have been corrected

CISWG II Example – Management

- (8) Establish IS Management Policies and Controls and Monitor Compliance
  - Percentage of IS Program Elements for which policies have been developed and implemented
  - Percentage of staff assigned responsibilities for IS policies who have acknowledged accountability for their responsibilities in connection with these responsibilities

CISWG II Example - Management

- (9) Assign IS Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges
  - Percentage of job performance reviews that include evaluation of IS responsibilities and IS policy compliance
  - Percentage of people with high level system privileges who have undergone background checks

CISWG II Example - Management

- (10) Assess Information Risks and Actively Manage Risk Mitigation
  - Percentage of critical information assets and information-dependent functions and objectives for which formal risk assessments have been performed and documented in accordance with policy
  - Percentage of identified risks that have a defined risk mitigation plan against which status is reported in accordance with policy

CISWG II Example- Technical

- (18) User Identification and Authentication
  - Percentage of active user ID's assigned to only one person
  - Percentage of systems and applications that perform authentication (e.g., password) policy verification upon establishing a new password
  - Percentage of active user passwords that are set to expire in accordance with policy

CISWG II Example - Technical

- (18) User Identification and Authentication (Cont'd)
  - Percentage of active user passwords that are set to expire in accordance with policy
  - Percentage of systems with critical information assets that use stronger authentication than ID's and passwords in accordance with policy

CISWG II Example - Technical

- (20) User Privileges
  - Percentage of active user accounts that have been reviewed for justification of current access privileges in accordance with policy
  - Percentage of systems and applications where assignment of user privileges is in compliance with the policy that specifies role-based access privileges

CISWG II Example - Technical

- (21) Configuration Management
  - Percentage of systems for which configuration settings have been implemented as required by policy
  - Number of deviations from approved system configurations
  - Percentage of systems that are continuously monitored for configuration policy with out-of-compliance alarms or reports

What to do right now

- Make sure that appropriate attention is being given to the program elements
- Implement the metrics that measure what is important to the security of your information
- Prioritize your efforts/expenditures based on cost/benefit considerations

Finally…

- Cybersecurity is a comprehensive challenge
- Work the near-term and long-term concurrently
- It's about people, process and technology, so balance your energies among these areas
- View it as an opportunity for organizational improvement, not just regulatory compliance


http:www.cisecurity.org
ckreitner@cisecurity.org
the CENTER for
INTERNET SECURITY